STEVEN G. KALAR
Federal Public Defender
DAVID W. RIZK
Assistant Federal Public Defender
450 Golden Gate Avenue
San Francisco, CA 94102
Telephone: 415.436.7700
Facsimile: 415.436.7706
David_Rizk@fd.org

Counsel for Defendant BOHANNON

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. WESLEY BOHANNON, Defendants.	Case No. CR 19-00039 CRB **DEFENDANT'S MOTION TO SUPPRESS AND REQUEST FOR EVIDENTIARY HEARING** **REDACTED COPY**

TO: THE UNITED STATES OF AMERICA, PLAINTIFF; DAVID ANDERSON, UNITED STATES ATTORNEY; AND DAN KARMEL, ASSISTANT UNITED STATES ATTORNEY

PLEASE TAKE NOTICE that on December 17, 2020, at 1:30 p.m., or as soon thereafter as the matter may be heard, in the courtroom of the Honorable Charles R. Breyer, counsel for defendant Wesley Bohannon will move this Court for entry of an order requiring the government to produce documents related to its investigation in this case. This motion is based on the Fourth Amendment's warrant requirement, all relevant case law and statutory authority, the following memorandum of points

and authorities, any reply memorandum, and any oral argument made at the motion hearing. Should any disputed issue of material fact arise with respect to this motion to suppress, Mr. Bohannon further moves this Court for an evidentiary hearing.

\\

\\

\\

\\

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

I. INTRODUCTION

Defendant Wesley Bohannon moves to suppress the fruits of certain searches that violated the Fourth Amendment. The National Center for Missing and Exploited Children ("NCMEC"), which is a government entity and agent, and Microsoft Online Services ("Microsoft"), which acted as a government agent, conducted unconstitutional, warrantless searches of Mr. Bohannon's Microsoft OneDrive file-hosting account and files on behalf of the government, leading to the institution of this case for possession of child pornography.[1] Microsoft and NCMEC forwarded the results of their searches, as well as additional information NCMEC's own investigators found, to San Francisco Police Department (SFPD) Sergeant Christopher Servat. Also without a warrant, Sgt. Servat reviewed a single image flagged by Microsoft and NCMEC and determined it to be child pornography. He then applied for a state search warrant for the account information and all of the contents of the identified OneDrive account. In the state search warrant application, Sgt. Servat relied on tainted information obtained from NCMEC and Microsoft's unlawful and warrantless searches, including his own review of the sole flagged image. *However*, even if the Court rejects the finding that Microsoft and/or NCMEC were acting as agents of the government, the state search warrant still must be invalidated because Sgt. Servat omitted and misrepresented critical information, without which probable cause could not have been established. In particular, Sgt. Servat's probable cause statement failed to state *when or how Microsoft identified the alleged child pornography*. Sgt. Servat's declaration also failed to set forth any facts whatsoever to establish probable cause that *child pornography would likely be stored indefinitely on a paid file-hosting service irrespective of the date of discovery (since none was disclosed)*, let alone for any particular period of time, long or short. Ninth Circuit law clearly forbids a finding of probable cause under these circumstances and no objectively reasonable officer could think otherwise. *See United States v. Lacy*, 119 F.3d 742, 745-745 (9th Cir. 1997).

\\

[1] For purposes of this motion only, Mr. Bohannon presumes the following alleged facts are true, based on the discovery provided by the government. Such argument does not constitute an admission of any allegation in this case.

Individually and collectively, these facts require suppression of the fruits of the unconstitutional searches Mr. Bohannon's OneDrive account.

II. FACTUAL BACKGROUND

A. Microsoft searches Mr. Bohannon's digital files and submit reports on his accounts to NCMEC, which forwards the search results to SFPD.

On December 6, 2017, Microsoft learned that a user had uploaded alleged child pornography image onto a Microsoft OneDrive account. Rizk Decl., Ex. A (CyberTip No. 26157907) at WSB-192. OneDrive is a file-hosting service owned by Microsoft; users can upload data files to OneDrive and then access those file on multiple devices.[2] NCMEC received a report from Microsoft on December 14, 2017. *Id.* at WSB-192. Microsoft reported a numeric user name and IP address associated with the OneDrive account. *Id.* at WSB-190. To this information, NCMEC added additional information from its own investigation concerning the owner of the IP address, which it identified as the California State University, Office of the Chancellor. *Id.* at WSB-194. NCMEC forwarded the report to local law enforcement. *Id.* at WSB-198. It appears from the CyberTip report that Microsoft identified the image using a system called PhotoDNA. *Id.* at WSB-193. It is not clear from the CyberTip report or the discovery provided in this case whether the image was ever reviewed by a Microsoft employee before it was sent to NCMEC and SFPD. Although not explained in the CyberTip report or set forth in the warrant application, PhotoDNA is a system developed by Microsoft and donated to NCMEC to assist law enforcement.[3] According to Microsoft: "Microsoft has also provided PhotoDNA for free to law enforcement, primarily through forensic tool developers. PhotoDNA has been widely incorporated into innovative visual image and forensic tools used by law enforcement around the world." *Id.* Microsoft describes the system as follows: "PhotoDNA creates a unique digital signature (known as a 'hash') of an image which is then compared against signatures (hashes) of other photos to find copies of the same image." *Id.*

---

[2] *See* Microsoft OneDrive: Personal cloud storage, *at* https://onedrive.live.com/about/en-us/ (October 9, 2020).

[3] Microsoft PhotoDNA, *at* https://www.microsoft.com/en-us/photodna (October 9, 2020) ("Microsoft donated PhotoDNA to the National Center for Missing & Exploited Children (NCMEC)").

B. SFPD obtains a state search warrant for all account and subscriber information, as well as the contents of Mr. Bohannon's Microsoft account.

Following receipt of the CyberTip report, on January 4, 2018, Sgt. Servat applied for and obtained a search warrant to Microsoft for

> OneDrive account for User ID 1759221994097800. For the following;
> -All account information, Subscriber names, user names, and other identities
> -Email addresses, telephone numbers, and other contact information associated with account
> -Length of service of account
> -IP connection log history of user access from 07/01/2017 and 01/03/2018, and IP log information relating to account creation
> -All content in OneDrive account
> -All images, links, videos, [sic] uploaded and saved on account from 07/01/2017 and 01/03/2018

See Rizk Decl., Ex. B (WSB-0056-60) at WSB-55-57. The probable cause statement stated that Microsoft had reported child pornography on a Microsoft OneDrive account associated with a particular user ID, as well as an IP address, which Sgt. Servat stated "geo-located to San Francisco." *Id.* at WSB-59. The warrant also explained that

> OneDrive is a file-hosting service operated by Microsoft as part of its suite of online services. It allows users to store files as well as other personal data like Windows settings or Bitlocker recovery keys in the cloud. Files can be synced to a PC and accessed from a web browser or a mobile device, as well as shared publicly or with specific people.
>
> OneDrive offers 5 GB of storage space free of charge, additional storage can be added either separately or through subscriptions to other Microsoft services.

Id. However, the probable cause statement did not set forth any facts describing *when or how Microsoft had identified the child pornography, or when or how Microsoft had associated it with the OneDrive account, user ID, or IP address*. Relatedly, *Sgt. Servat also did not provide any information or facts to suggest that child pornography might be stored electronically indefinitely*, let alone stored for long periods of time, in a monthly paid[4] file-hosting service, such as Microsoft OneDrive. Indeed, *Sgt. Servat provided no averments whatsoever concerning the nature of electronically-stored contraband, or the habits of those who collect it.* Finally, Sgt. Servat also did not inform the Court that NCMEC had reported the IP address was owned by California State University, Office of the

[4] *See* Microsoft365 OneDrive – Compare OneDrive plans (describing monthly payment plans), *available at* https://www.microsoft.com/en-us/microsoft-365/onedrive/compare-onedrive-plans?activetab=tab%3aprimaryr1 (October 9, 2020).

Chancellor. No protocol for sifting the requested data was proposed. The warrant was signed without modification by the Superior Court on January 4, 2018. *Id.* at WSB-0057.

C. SFPD obtains a state search warrant for Mr. Bohannon's person, property and effects, including digital devices and their contents, as well as his bedspace and locker.

Approximately two months later, on March 7, 2018, Sgt. Servat received the search results from Microsoft. Rizk Decl., Ex. C (WSB-0045-52) at WSB-59. Sgt. Servat states that he reviewed the contents of the OneDrive account and discovered approximately five hundred images of child pornography, among other materials, which he would later use to obtain a second state search warrant.[5] *Id.* at WSB-0046.

D. Mr. Bohannon agrees to meet with SFPD, is arrested at UCSF, agrees to a voluntary interview, invokes his right to counsel, and is charged by the District Attorney.

On March 13, 2018, SFPD contacted Mr. Bohannon to request a meeting. Rizk Decl., Ex. C at WSB-0048. Mr. Bohannon agreed to meet Sgt. Servat and another officer and told them that he would be at a medical appointment at UCSF's Acute Care Clinic on the requested date, March 15, 2018. *Id.* at WSB-0048-49. Sgt. Servat and other officers arrested Mr. Bohannon at the UCSF Parnassus campus and seized a cell phone and a laptop found on his person, which later revealed additional child pornography when searched. *Id.* at WSB-0048-49. Mr. Bohannon agreed to be voluntarily interviewed by Sgt. Servat, and acknowledged that he was a sex offender. *Id.* When told by Sgt. Servat of the child pornography associated with the OneDrive account, Mr. Bohannon immediately invoked his right to counsel. *Id.* at WSB-49-50. Mr. Bohannon was charged and booked at San Francisco General Hospital because he was declined at the San Francisco Jail for health reasons, and subsequently released on bail by the Superior Court with electronic monitoring. Rizk Decl., ¶ 8.

[5] Mr. Bohannon reserves the right to challenge that second warrant, should the Court invalidate the warrant challenged herein. Mr. Bohannon also reserves the right to challenge additional warrants Sgt. Servat obtained for information from Google, Inc., which raise complex technical issues that are distinct from those addressed here and will likely require expert testimony.

E. Mr. Bohannon is indicted federally for one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(b) and (b)(2).

On January 22, 2019, Mr. Bohannon was indicted by a federal grand jury for one count of possession of child pornography in connection with the materials found at the time of his arrest on March 15, 2018. *See* ECF No. 1. Mr. Bohannon was re-arrested federally, arraigned, and released on stringent conditions, including electronic monitoring, by Chief Magistrate Judge Spero, on March 19, 2019. *See* ECF Nos. 4, 6. Since that time, Mr. Bohannon has had no violations on pretrial release. Since the beginning of the pandemic, he has primarily been sheltering-in-place as he is particularly vulnerable to COVID-19, due to his chronic obstructive pulmonary disease ("COPD") and other health conditions. Rizk Decl., ¶ 9.

F. NCMEC is a government entity that is statutorily obligated to receive reports regarding child pornography and distribute them to federal and local law enforcement.

Although the Ninth Circuit has never addressed the issue, NCMEC has been deemed by other courts to be both a government actor and a government entity. *United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016), *reh'g denied* (Oct. 4, 2016); *see also, United States v. Keith*, 980 F.Supp.2d 33, 40-43 (D. Mass. 2013). NCMEC's two authorizing statutes—18 U.S.C. § 2258A and 42 U.C.S. §5773(b)—mandate its collaboration with federal, state, and local agencies "in over a dozen ways." *Ackerman*, 831 F.3d at 1296. NCMEC is, for instance, statutorily obligated

> to operate the official national clearinghouse for information about missing and exploited children, to help law enforcement locate and recover missing and exploited children, to "provide forensic technical assistance . . . to law enforcement" to help identify victims of child exploitation, to track and identify patterns of attempted child abductions for law enforcement purposes, to "provide training . . . to law enforcement agencies in identifying and locating non-compliant sex offenders," and . . . to operate the CyberTipline as a means of combating Internet child sexual exploitation.

Id. (citing 42 U.S.C. § 5773(b)). Significantly, NCMEC is also funded heavily by the federal government. In the period relevant to this case, 2016-18, the U.S. Department of Justice funded NCMEC to the tune of $28.3 million annually (constituting the largest share of funding distributed by

the Department's Missing and Exploited Children program).[6]

NCMEC's rights and responsibilities regarding child pornography are specific. Service Providers such as Microsoft are required to report any known image of child pornography to NCMEC, rather than federal or local law enforcement. 18 U.S.C. §§ 2258A(a)(1) & (g)(2)(B)(i). Indeed, the U.S. Department of Justice lists NCMEC as the appropriate authority to which to report any "incident involving the possession, distribution, receipt, or production of child pornography."[7] Such reports may include "the identity of any individual who appears to have violated a Federal law" involving child pornography, "the electronic mail address, Internet Protocol address, uniform resource locator, or any other identifying information, including self-reported identifying information" for that individual, his or her geographic location, and any image of suspected child pornography relating to the incident underlying the report. 18 U.S.C. § 2258A(b). If a service provider like Microsoft fails to make a report, it faces a $150,000 fine for a first offense, and a $300,000 fine for each offense thereafter. 18 U.S.C. § 2258A(e).

When NCMEC confirms that it has received a report from a service provider, it "must treat that confirmation as a request to preserve evidence issued by the government itself," *Ackerman*, 831 F.3d at 1297, is permitted to "receive [any attached child pornography] knowingly and to review its contents intentionally," *id.*, and must subsequently "transmit [that] report[], including relevant images and information, to the appropriate international, Federal, State or local law enforcement agency for investigation," 42 U.S.C. § 5773. These are rights and responsibilities that "Congress has extended to NCMEC alone . . . specifically to assist or support law enforcement agencies in administration of criminal justice functions." *Ackerman*, 831 F.3d at 1297 (citation and quotations marks omitted). By contrast, and unlike NCMEC, private parties would ordinarily risk prosecution by knowingly receiving and reviewing child pornography. *See* 18 U.S.C. § 2252A(a)(2) (receipt); *id.* § 2252A(a)(5)(B)

---

[6] *See* Congressional Research Service, The Missing and Exploited Children's (MEC) Program: Background and Policies (July 29, 2019), pp. 7 (Table 1), *at* https://fas.org/sgp/crs/misc/RL34050.pdf (July 14, 2020).

[7] *See* U.S. Department of Justice – Report Violations, *at* https://www.justice.gov/criminal-ceos/report-violations (October 9, 2020).

(possession). Notably, however, NCMEC is authorized to provide technical information from the CyberTip reports NCMEC generates—*i.e.*, "hash values or other unique identifiers associated with a specific visual depiction, including an Internet location and any other elements provided in a CyberTipline report," except child pornography images—to service providers such as Microsoft to enable "the provider to stop the online sexual exploitation of children." 18 U.S.C. § 2252C(a)(1) & (a)(2). No other private parties, other than service providers, are authorized to receive such information from NCMEC to assist in enforcement activity. *Id.*

G. Microsoft provides substantial financial and technical support to NCMEC, including the specific technology, PhotoDNA, that was used to search Mr. Bohannon's OneDrive account in this case.

NCMEC has a long and unique history of partnership and close cooperation with Microsoft. The company has long provided NCMEC financial and technical support. Microsoft is a founding member of NCMEC's public-private Technology Coalition as well as its Financial Coalition Against Child Pornography.[8] According to NCMEC: "The Technology Coalition [was] funded within NCMEC to develop and deploy technology solutions that disrupt the ability of predators to use the Internet to exploit children or traffic in child pornography."[9] Its purpose is "to enhance knowledge sharing among industry participants, *improve law enforcement tools*, and research perpetrators' technologies in order to enhance industry efforts and build solutions." *Id.* (emphasis added). In Microsoft's words: "The Coalition will work to identify and implement advanced technologies to combat child exploitation, and *to facilitate information-sharing and cooperation among industry and law enforcement*." *See supra* at

[8] Press Release, "Statement from Microsoft on Establishment of Technology Coalition within National Center for Missing and Exploited Children," June 27, 2006, (emphasis added) *available at* https://news.microsoft.com/2006/06/27/statement-from-microsoft-on-establishment-of-technology-coalition-within-national-center-for-missing-and-exploited-children/ (October 9, 2020). *See also* Government Technology, "Financial and Internet Industries To Combat Internet Child Pornography," March 28, 2006, *available at* https://www.govtech.com/security/Financial-and-Internet-Industries-To-Combat.html (October 9, 2020). *See also* NCMEC – Our Corporate Partners, *available at* https://www.missingkids.org/supportus/our-corporate-partners (October 9, 2020).

[9] Press Release, "Google Joins Industry-Wide Movement to Combat Child Pornography," https://www.icmec.org/press/google-joins-industry-wide-movement-to-combat-child-pornography/ (October 9, 2020).

n. 5 ("Statement from Microsoft…") (emphasis added).

Although NCMEC is primarily financed by the U.S. Department of Justice, Microsoft also supports it financially. In the past, NCMEC has refused to say how much in private donations it receives. *Ackerman*, 831 F.3d at 1299. However, public records indicate that Microsoft has made donations to NCMEC worth millions of dollars over the years, including in the form of massive technology transfers.[10] For example, in 2010, Microsoft publicly stated that it had donated more than $3.1 million worth of technology to NCMEC in total. *Id.*

Most significantly for present purposes, Microsoft developed PhotoDNA—the very technology that Microsoft apparently used in this case—and then donated it to NCMEC. PhotoDNA was developed by Microsoft. *See supra* at n.2. [redacted]

[10] Press Release, "Technology in Action: National Center for Missing & Exploited Children," August 23 2020, *available at* https://blogs.microsoft.com/on-the-issues/2010/08/23/technology-in-action-national-center-for-missing-exploited-children/ (October 9, 2020); *see also supra at* n. 10 ("Statement from Microsoft …" announcing initial contributions totaling $1 million to NCEMC's Technology Coalition).

[redacted] Thus, Microsoft and NCMEC shared joint access and control over the very technology that was used by the company and NCMEC to conduct the initial warrantless searches of Mr. Bohannon's OneDrive account.

III. ARGUMENT

A. The government bears the burden of proving that the warrantless searches fell within an exception to the Fourth Amendment's warrant requirement.

"The Fourth Amendment provides in relevant part that '[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.'" *United States v. Jones*, 132 S. Ct. 945, 949 (2012) (quoting U.S. Const. amend. IV). The digital information stored on Mr. Bohannon's OneDrive account implicates the Fourth Amendment's specific guarantee of an individual's right to be secure in his "papers." This follows from the fact that information stored on cloud servers, like the cloud servers supporting Microsoft's products, includes "the same kind of highly sensitive data one would have in 'papers' at home." *United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013); *see also, e.g., United States v. Chan*, 830 F. Supp. 531, 534 (N.D. Cal. 1993) ("The expectation of privacy in an electronic repository for personal data is . . . analogous to that in a personal address book or other repository for such information.").

Cloud servers such as Microsoft's OneDrive account service are, like laptops, iPads, cell phones, and other instruments of modern information storage, "simultaneously offices and personal diaries," private, digital compartments that "contain the most intimate details of our lives." *Cotterman*, 709 F.3d at 965; *see also Riley v. California*, 134 S. Ct. 2473, 2491 (2014) (Fourth Amendment protects cell phones in part because of their "immense storage capacity," resulting in part from their access to information stored "in the cloud"); *United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009) ("Searches of computers . . . often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."). Because cloud servers contain the same

intensely intimate information as their physical counterparts, they trigger the same constitutional protections. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (emphasizing that evolving technology cannot be allowed to "erode the privacy guaranteed by the Fourth Amendment").

1. NCMEC and Microsoft, acting as government agents, or as a government entity and its agent, respectively, conducted unconstitutional searches of Mr. Bohannon's OneDrive account.

A "search" occurs, for Fourth Amendment purposes, in two circumstances. It occurs, first, when the government or an entity acting as a government agent infringes "an expectation of privacy that society is prepared to consider reasonable." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). It occurs, second, when the government or its agent intrudes or trespasses upon a constitutionally protected area—"persons, houses, papers, [or] effects"—to obtain information. *United States v. Jones*, 565 U.S. 400, 405 (2012); *see also Lyall v. City of Los Angeles*, 807 F.3d 1178, 1185 (9th Cir. 2015) ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." (citation and quotation marks omitted) (emphasis in original)); *United States v. Lundin*, 817 F.3d 1151, 1158 (9th Cir. 2016) (crediting *Jones*' property-right conception of Fourth Amendment analysis).

Under either theory, Mr. Bohannon's OneDrive account was subjected to at least three warrantless searches: (1) Microsoft's original search of the files in his OneDrive account with the use of PhotoDNA; (2) NCMEC's subsequent search of the image forwarded by Microsoft to NCMEC; and (3) Sgt. Servat's final search of the same image. While the conduct of a private citizen or organization ordinarily would not be attributable to the state, both Microsoft and NCMEC were acting as government agents when they searched the contents of Mr. Bohannon's OneDrive account. *See George v. Edholm*, 752 F.3d 1206, 1215 (9th Cir. 2014) ("A private party's search may be attributed to the state when 'the private party acted as an instrument or agent of the Government' in conducting the search." (quoting *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 614 (1989)); *Keith*, 980 F.Supp.2d at 40-43 (holding that NCMEC was acting as a government agent under similar circumstances). NCMEC,

moreover, also qualifies as a government entity. *See Ackerman*, 831 F.3d at 1295-1301 (holding that NCMEC is a government entity).

In cases where a search was allegedly conducted by a non-governmental actor, the question of whether the Fourth Amendment applies to that search requires consideration of "(1) the government's knowledge and acquiescence, and (2) the intent of the party performing the search." *United States v. Walther*, 652 F.2d 788, 192 (9th Cir. 1981). The Ninth Circuit applied this test in *Walther*, and concluded that the employee who performed the search had acted as an agent of the government. *Id.* at 793. In that case, the employee who performed the challenged search worked for an airline named Western Airlines. *Id.* at 789. While so employed, he opened a case and found white powder, and contacted the DEA. *Id.* The case was then repackaged. *Id.* This employee had opened packages in the past and made prior reports to the DEA as a paid informant. *Id.* at 790. The Ninth Circuit considered whether that individual employee was acting as a government agent in the context of that search, and concluded that he was. *Id.* at 793.

Applying the same two-factor test in *United States v. Ackerman*, 831 F.3d 1292, 1296-97 (10th Cir. 2016), the Tenth Circuit, in an opinion authored by then-Judge Neil Gorsuch, concluded that NCMEC functioned as a government entity for purposes of the Fourth Amendment, rendering its actions subject to the Fourth Amendment's warrant requirement. *See Ackerman*, 831 F.3d at 1296; *see also United States v. Rosenschein*, No. 16-CR-4571, 2019 WL 2298810 (D.N.M. May 30, 2019) (finding NCMEC is a member of the prosecution team sufficient to trigger discovery obligations under Rule 16). Here, there is no question that the government, at least through the government entity NCMEC, knew of and acquiesced in Microsoft and NCMEC's joint conduct. The government not only collaborates with both organizations to ferret out child pornography, but it also statutorily mandates their participation. *See* 18 U.S.C. § 2258A. Critically, here, the record shows that Microsoft and NCMEC jointly developed, maintain, and controlled the very technology that was used to conduct the search in this case. And, just as was the case for the informant in *Walther*, Microsoft and NCMEC have a long track record of assisting the government—and NCMEC is even primarily financed by the

Department of Justice. *Walther*, 652 F.2d at 790. Indeed, Microsoft's and NCMEC's actions and public statements, referenced above, indicate that they collaborated together, including on the technology that is at issue here and was used to search Mr. Bohannon's account, for the express of assisting law enforcement. *See supra* at section II.G. In this case, both Microsoft and NCMEC assumed a law enforcement role by proactively investigating the Mr. Bohannon's account. Microsoft actively searched his files, and reported his IP address, while NCMEC took the affirmative steps of investigating the IP address and forwarding information concerning the location and owner of the IP address to SFPD.

Mr. Bohannon acknowledges, as he must, that the weight of precedent in this District and across the country does not support the view that Microsoft, in particular, has acted as a government agent in similar circumstances.[11] None of these cases, however, is exactly on all fours with the parties and the technology, jointly developed between Microsoft and NCMEC, that is at issue here. Further, the Ninth Circuit has yet to weigh in on this emerging area of the law. Mr. Bohannon therefore respectfully requests a ruling to secure his rights.

2. The government cannot establish that any exception to the Fourth Amendment's warrant exception applies.

It is well established that any warrantless search is *per se* unreasonable, subject only to a few well-delineated exceptions. *United States v. Scott*, 705 F.3d 410, 416 (9th Cir. 2012); *United States v. Hawkins*, 249 F.3d 867, 872 (9th Cir. 2001). For that reason, "[t]he burden of proving that a warrantless search or seizure falls within an exception to the warrant requirement is on the government." *Scott*, 705 F.3d at 416 (citing *Hawkins*, 249 F.3d at 872); *see also United States v. Johnson*, 936 F.3d 1082, 1084 (9th Cir. 1991) ("The government bears the burden of justifying a

[11] *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013); *United States v. Cameron*, 699 F.3d 621 (1st Cir. 2012); *United States v. Richardson*, 607 F.3d 357, 367 (4th Cir. 2010); *United States v. Wolfenbarger*, 16-CR-00519-LHK, 2019 WL 6716357 (N.D. Cal. Dec. 10, 2019); *United States v. Viramontes*, 16-CR-508-EMC, ECF No. 62 (N. D Cal. Nov. 14, 2017); *United States v. Lien*, 16-CR-393-RS, 2017 U.S. Dist. LEXIS 188903 (N.D. Cal. May 10, 2017).

warrantless search."). The government must prove that any exception applies by a preponderance of the evidence. *United States v. Vasey*, 834 F.2d 782, 785 (9th Cir. 1987).

Mr. Bohannon invites the government to demonstrate that each of the presumptively unreasonable searches in this case was lawful. He submits, however, that the government will be unable to meet its burden and therefore that all evidence obtained as a result of these Fourth Amendment violations must be suppressed as "fruit of the poisonous tree." *See Wong Sun v. United States*, 371 U.S. 471, 488 (1963); *United States v. Washington*, 490 F.3d 765, 775 (9th Cir. 2007) (quoting *Wong Sun*, 371 U.S. at 488) ("[E]vidence obtained subsequent to a violation of the Fourth Amendment is tainted by the illegality and is inadmissible . . . unless the evidence obtained was 'purged of the primary taint.'"); *United States v. Davis*, 332 F.3d 1163, 1170-71 (9th Cir. 2003) ("[T]he standard articulated in *Wong Sun* remains the relevant test.").

B. SFPD's state search warrant application failed to establish probable cause, and therefore the fruits of the search must be suppressed.

The state search warrant obtained by Sgt. Servat to search Mr. Bohannon's OneDrive account also violated the Fourth Amendment for several reasons. First, as an initial matter, the statement of probable cause filed in support of the warrant relied on information obtained by Sgt. Servat from Microsoft's and NCMEC's unlawful warrantless searches. Second, and even more clearly fatal, the probable cause statement did not set forth any facts describing *when or how Microsoft had identified the child pornography, or when or how Microsoft had associated it with the OneDrive account, user ID, or IP address* that was reported. Without this key information, probable cause could not possibly be established. Third, and closely relatedly to this first omission, the probable cause statement failed to establish probable cause that contraband would likely be found in the place to be searched because *Sgt. Servat did not provide any information or facts to establish that child pornography would be stored indefinitely (without regard to the date of discovery) on a paid file-hosting service*, let alone stored for long periods of time. Finally, the probable cause statement also omitted information about the reported IP address, and the application failed to propose any protocol for filtering the entire contents of Mr. Bohannon's account. Both individually and collectively, these facts require

suppression of the fruits of the search of Mr. Bohannon's OneDrive account.

1. The probable cause statement relied primarily on the fruits of Microsoft, NCMEC, and SFPD's presumptively unconstitutional searches.

As an initial matter, all fruits of the warrant search of Mr. Bohannon's OneDrive accounts must be suppressed because the warrant itself was tainted fruit from the initial warrantless searches by Microsoft and NCMEC, which, as discussed above, violated the Fourth Amendment. *See, e.g., Murray v. United States*, 487 U.S. 533, 536-42 (1988) (exclusionary rule applies to warrant if information from prior illegal search was material to magistrate's decision to issue it). Here, all of the information provided in support of the state search warrant application was provided by Microsoft and NCMEC to Sgt. Servat; without such, there was no information whatsoever to justify a finding of probable cause. Moreover, "the good-faith exception may not be invoked when 'the search warrant was issued in part on the basis of evidence obtained from an illegal search.'" *United States v. Artis*, 919 F.3d 1123, 1133 (9th Cir. 2019) (quoting *United States v. Wanless*, 882 F.2d 1459, 1466-67 (9th Cir. 1989)).

2. The probable cause statement failed to include any facts concerning when or how Microsoft identified the contraband, or why electronically-stored child pornography would likely be found in a paid file-hosting account indefinitely.

A warrant application that fails entirely to provide the most basic information—when or how a reporting third-party discovered contraband, and why the contraband would likely still be found in the place to be searched—cannot establish probable cause. Without establishing the time at which the contraband was discovered or any basic facts concerning the nature of electronically-stored child pornography and the habits of those who collect it, the warrant application effectively asks the Court to simply assume that the suspected contraband was preserved indefinitely on a paid file-storage service, without providing any context or justification for that conclusion. Supreme Court and Ninth Circuit law clearly forbids the Court from finding probable cause in these circumstances.

Before a search warrant issues, the government must "establish by sworn evidence presented to a magistrate that probable cause exists to believe that an offense has been committed and that items related to that offense . . . will be found on the premises sought to be searched at the time the warrant is issued." *Rabe*, 848 F.2d at 997 (9th Cir. 1988); *see also Illinois v. Gates*, 462 U.S. 213, 238 (1983).

The probable cause determination depends upon the "totality of the circumstances," *Gates*, 462 U.S. at 230-31, and "applies with equal force to cases involving child pornography on a computer," *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006). Probable cause in this context means a "fair probability that contraband or evidence is located in a particular place." *Gates*, 462 U.S. at 231. That probability is based on an affidavit, which must present enough information for a magistrate independently to determine probable cause. The magistrate's determination "cannot be a mere ratification of the bare conclusion of others." *Gates*, 462 U.S. at 230.

In *United States v. Lacy*, the Ninth Circuit explained the test for staleness in the context of an investigation of electronically-stored child pornography: "'We evaluate staleness in light of the particular facts of the case and the nature of the criminal activity and property sought.'" 119 F.3d at 745 (quoting *United States v. Pitts*, 6 F.3d 1366, 1369 (9th Cir. 1993). ""The mere lapse of substantial amounts of time is not controlling in a question of staleness.'" *Id.* (quoting *United States v. Dozier*, 844 F.2d 701, 707 (9th Cir. 1988)). "The information offered in support of the application for a search warrant is not stale if 'there is sufficient basis to believe, based on a continuing pattern or other good reasons, that the items to be seized are still on the premises.'" *Id.* at 745-46 (quoting *United States v. Gann*, 732 F.2d 714, 722 (9th Cir. 1984)). However, the Ninth Circuit specifically warned that, "[*w*]*e are unwilling to assume that collectors of child pornography keep their materials indefinitely*," *id.* at 746 (emphasis added), and then went on to require that the supporting declaration must provide specific, "good reasons" to believe that the contraband would likely be found in the place to be searched even after a delay. *Id.* As this Court is no doubt aware, it has now long been standard practice for investigators to include such averments to justify delays in the collection of electronic evidence. *See, e.g., United States v. Schesso*, 730 F.3d 1040, 1047 (9th Cir. 2013) (relying on affidavit swearing that "individuals who possess child pornography 'rarely, if ever, dispose of sexually explicit images of children' because these images are treated as 'prized possessions'").

In *Schesso*, for example, the Ninth Circuit made very clear that "law enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for

electronic evidence." *See* 730 F.3d at 1042. *Schesso* found probable cause for the search where the search warrant application: (1) described a video the defendant had downloaded and the agents had seen; (2) confirmed that the defendant had uploaded and distributed the video through a peer-to-peer network designed for sharing; (3) explained the operation of that network and described the storage capacity of the electronic evidence to be searched; (4) explained how the internet is generally used to distribute child pornography; and (4) identified the known characteristics of child pornography collectors. *Id.* at 1043. In *Lacy*, the Ninth Circuit similarly relied on an affidavit that specifically outlined the characteristics of child pornographer collectors to retain their collections for long periods of time. *Id.* at 745-46 ("Based on her training and experience as a Customs agent, the affiant explained that collectors and distributors of child pornography value their sexually explicit materials highly, 'rarely if ever' dispose of such material, and store it 'for long periods' in a secure place, typically in their homes."). *See also United States v. Greathouse*, 297 F. Supp. 2d 1264, 1270-73 (D. Or. 2003) (months-long delay too long given "the limited incriminating evidence, the absence of any evidence of intervening criminal activity, the absence of any evidence that [the target] was a pedophile, and the fact that computer equipment becomes obsolete very quickly" and given that "no explanation or justification for such a significant delay was ever offered").

Here, applying the Ninth Circuit's test in *Lacy* and guidance from *Schesso*, it is abundantly clear that Sgt. Servat's minimal statement falls far short of establishing probable cause. The defense has been unable to locate any case where law enforcement failed entirely to identify *when*, let alone *how*, contraband was detected in a prosecution of electronically-stored child pornography, such as this. Without knowing *when* Microsoft learned of the child pornography, the reviewing court simply could not make any determination concerning the likelihood that it would still be found in the OneDrive account. To the extent Sgt. Servat may attempt to rely on his statement that he received the CyberTip on January 2, 2018, that is immaterial and does not assist to establish probable cause because there are no facts recited to link the timing his receipt of the CyberTip report to the time of Microsoft's original discovery. As Sgt. Servat was aware (but did not inform the Superior Court), CyberTip reports may

languish for months or years before an investigator receives or follows up on them. Indeed, in this very case, Sgt. Servat applied for a separate state search warrant based on a CyberTip report, dated May 24, 2017, that he received nearly a year and a half later, on September 18, 2018. Rizk Decl. ¶ 10. Thus, the time of his receipt of the CyberTip report does not meaningfully inform as to the time Microsoft originally discovered the child pornography.

The failure to provide any information concerning *how* Microsoft discovered the child pornography further compounds the problem. In particular, Sgt. Servat did not convey to the Court that Microsoft apparently used PhotoDNA to discover the contraband. Nor did he provide any information concerning the reliability of PhotoDNA that would have been material to the probable cause determination. *See infra* at section III.B.3. Sgt. Servat also failed to relate that it was not clear from the CyberTip whether any Microsoft employee had actually viewed the image to confirm that it consisted of child pornography prior to sending it on to NCMEC and law enforcement. Similarly, Sgt. Servat provided no information concerning how Microsoft linked the image to the numeric user name and IP address associated with the OneDrive account. As noted above, nor did Sgt. Servat provide any information about the reporting process from Microsoft to NCMEC. Without any of this critical contextual information, the reviewing court could not have fairly assessed the reliability of the link between, on the one hand, the single image—which was found at some unknown time, and could have even been the result of inadvertence or mistake and hence not even criminal—and, on the other, the likelihood that the OneDrive account SFPD sought to have searched would contain additional evidence or contraband. The fact that only a single image was found thus further undermines any conclusion that contraband would likely be found in the account, since there was no indication of a larger, and possibly persistent, collection, let alone clearly criminal activity. Indeed, no other evidence concerning the profile of a child pornography collector or sex offender or sex offense, was provided. The complete absence of these very basic contextual averments is in stark contrast to those detailed declarations that have been upheld under similar circumstances by the Ninth Circuit. *See, e.g.*, *United States v. Hay*, 231 F.3d 630, 635-36 (9th Cir. 2000).

Finally, the probable cause statement also did not set forth any information or facts to establish that that child pornography would likely be stored *indefinitely* (without regard to the date of discovery), let alone stored for long periods of time, on a paid file-hosting service such as Microsoft's OneDrive platform. Without a discovery date, or that basic background information, the warrant is plainly invalid. The Ninth Circuit's case law requires "good reasons" to justify a delayed electronic search that may include, at a minimum: "a continuing pattern" of criminal activity, *see Lacy*, 119 F.3d at 745-46 (quoting *Gann*, 732 F.2d 714); information explaining why child pornography collectors choose the particular form of electronic media at issue to permanently store contraband, *Hay*, 231 F.3d at 636; assurances that "even if [the defendant] had deleted the files, they could nevertheless be retrieved by a computer expert," *Hay*, 231 F.3d at 636; incriminating information about the profile of the particular individual associated with the account, *see United States v. Weber*, 923 F.2d 1338, 1344-45 (9th Cir. 1990) (discussing *United States v. Rabe*, 848 F.2d 994, 995 (9th Cir. 1988)); or information about "the known characteristics of child pornography collectors," including their habit of saving images and rarely disposing of them, *Schesso*, 730 F.3d at 1047. In *Hay*, the court expounded on the importance of these expert averments, which although seemingly just boilerplate, provide an essential basis for a finding of probable cause in child pornography investigations:

> [T]he boilerplate in [the detective's] affidavit provides context for Evans's transfer of 19 images to Hay's Internet address, and forms the basis upon which the magistrate judge could plausibly conclude that those files were still on the premises. It sets forth relevant background information about how child pornography is traded and distributed over the Internet: through use of chat rooms to establish contacts, followed by transmission or trading of images. It points out that the computer's ability to store images in digital form makes it an ideal repository for child pornography. The affidavit also explains that the computer has become one of the preferred methods of distribution of child pornographic materials and opines, based upon Galante's experience and that of colleagues, that searches and seizures of evidence from computers requires agents to seize all parts of a computer system to be processed later by a qualified computer expert. *See United States v. Gil*, 58 F.3d 1414, 1418 (9th Cir. 1995) ("[W]hen interpreting seemingly innocent conduct, the court issuing the warrant is entitled to rely on the training and experience of police officers."). In sum, the affidavit (including "boilerplate" based on the agents' experience), provides a substantial basis for the probable cause determination.

Hay, 231 F.3d at 636.

By contrast, the statement in this case contained *none of this standard supporting information*.

Here, the only other information Sgt. Servat provided was a generic description of Microsoft's OneDrive product, untethered to any explanation as to why it would likely be a permanent repository of child pornography. For example, it fails to explain why a *month-to-month paid service* would likely be a place for somebody to store a child pornography collection indefinitely; indeed, the prospect that the contraband could be deleted if Microsoft were not paid every month runs directly contrary to the experience of other law enforcement agents, discussed extensively in the case law, suggesting that offenders seek storage that is *secure* and *permanent*. *See, e.g., Lacy*, 119 F.3d at 745-46.

In sum, probable cause was clearly lacking in view of the glaring deficiencies in the probable cause statement, the state search warrant must be invalidated, and all of the fruits of the search of Mr. Bohannon's OneDrive account should be suppressed.

3. The probable cause statement intentionally or recklessly omitted information concerning how Microsoft identified the child pornography, including the reliability of PhotoDNA, and associated identifying information.

On top of the omissions discussed above, Sgt. Servat also intentionally or recklessly omitted key information concerning how Microsoft identified the child pornography and the associated account. In particular, Sgt. Servat concealed that the image had been identified by the PhotoDNA algorithm, neglected to explain how the algorithm works, and failed to state whether anyone at Microsoft contemporaneously viewed the image before forwarding it to NCMEC and ultimately law enforcement. This information was highly material to the reviewing court's probable cause determination to the extent that Sgt. Servat may rely upon the private search exception to justify his review of the image forwarded by Microsoft and NCMEC.[12] In particular, without any information about how Microsoft identified, reviewed, and reported information to NCMEC and law enforcement, the reviewing court could not evaluate whether Sgt. Servat's review of the image had impermissibly

[12] Mr. Bohannon adopts the premise that Sgt. Servat's conduct fell within the ambit of a private search only for the sake of argument, and only in the alternative, should the government raise the private search exception in an effort to justify Sgt. Servat's warrantless search of the reported image. As noted above, it is the government's burden to establish this exception, and should it attempt to do so, Mr. Bohannon reserves the right to raise additional arguments and make further submissions to show that the exception cannot be established and that Sgt. Servat's omissions in the warrant amounted to a *Franks* violation.

exceeded the scope of Microsoft's private search and thus violated the Fourth Amendment. *United States v. Jacobsen*, 466 U.S. 109, 119 (upholding private search exception where there was a "virtual certainty" that law enforcement's follow-on search would not reveal anything). The reckless failure to provide any information whatsoever how Microsoft's discovered the child pornography, and to what extent it reviewed the information before providing it to law enforcement, merits a hearing. *Franks v. Delaware,* 438 U.S. 154, 155-56 (1978).

Franks applies not only to falsehoods, but also to "deliberate or reckless *omissions* of fact which tend to mislead." *United States v. Stanert*, 762 F.2d 775, 781, *amended* 769 F.2d 1410 (9th Cir. 1985) (emphasis added).

> The use of deliberately falsified information is not the only way by which police officers can mislead a magistrate when making a probable cause determination. *By reporting less than the total story, an affiant can manipulate the inferences a magistrate will draw*. To allow a magistrate to be misled in such a manner could denude the probable cause requirement of all real meaning.

Id. (emphasis added). In the case of such intentional or reckless omissions, the court must review the warrant application "with the omitted information included" and determine whether the application would still establish probable cause. *United States v. DeLeon*, 979 F.2d 761, 764 (9th Cir. 1992). If not, the warrant is invalid and any fruits obtained via the warrant must be suppressed. To merit a *Franks* hearing, the Ninth Circuit "does not require clear proof of a deliberate or reckless omissions or misstatements at the pleading stage." *United States v. Gonzalez, Inc.*, 412 F.3d 1102, 1110 (9th Cir. 2005). "At this stage, all that is required is that the defendant make a substantial showing that the affiant intentionally or recklessly [misstated facts or] omitted facts required to prevent technically true statements in the affidavit from being misleading." *Stanert*, 762 F.2d at 781.

Finally, where a *Franks* claim is based upon material omissions from a warrant affidavit, a law enforcement officer acts with reckless disregard for the truth when he "withholds a fact in his ken that 'any reasonable person would have known that this was the kind of thing the judge would wish to know.'" *Wilson v. Russo*, 212 F.3d 781, 788 (3d Cir. 2000) (quoting *United States v. Jacobs,* 986 F.2d 1231, 1235 (8th Cir. 1993)); *see also id.* at 787 (acknowledging that "reckless disregard for the truth

means different things when dealing with omissions and assertions"); *Chism v. Washington*, 661 F.3d 380, 388 (9th Cir. 2011) ("The most commonsense evidence that the officer acted with at least a reckless disregard for the truth is that the omissions and false statements contained in the affidavit were all facts that were within [the officer's] personal knowledge.").

"The Fourth Amendment's proscriptions on searches and seizures are inapplicable to private action." *United States v. Tosti*, 733 F.3d 816, 821 (9th Cir. 2013) (citing *United States v. Jacobsen*, 466 U.S. 109, 113-14 (1984)). "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Id.* (quoting *Jacobsen*, 466 U.S. at 117). Rather, the Fourth Amendment "is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Id.* (quoting *Jacobsen*, 466 U.S. at 117). Accordingly, any "additional invasions of ... privacy by the government agent *must be tested by the degree to which they exceed[ ] the scope of the private search*." *Id.* (quoting *Jacobsen*, 466 U.S. at 115) (emphases added).

Although the foregoing principles from *Jacobsen* and *Tosti* generally apply here, those authorities are not dispositive here. The facts of this case are closer to *Walter v. United States*, 447 U.S. 649, 654-57 (1980). In *Walter*, a shipment was mistakenly received by the L'Eggs Hoisery company, and the receiving employees examined the exterior of the boxes, opened them, and found films. *Id.* at 652. The sides of the boxes contained suggestive drawing sand explicit descriptions of the contents of the films. *Id.* The FBI was summoned, and agents opened the boxes, found what were (then-considered) obscene films, and took the liberty of viewing them, all without a warrant. *Id.* In *Walter*, the court acknowledged that the labeling and descriptions may have provided the agents probable cause to obtain a warrant, but they failed to do so and instead simply open the boxes and viewed the films. *Id.* The labels themselves, of course, could not have sustained a conviction because they didn't amount to obscenity. *Id.* "Further investigation—that is to say, a search of the contents of the films—was necessary to obtain the evidence which was to be used at trial." *Id.* "Prior to the Government screening, one could only draw inferences about what was on the films." *Id.* The agent's warrantless review of

the images constituted "a significant expansion of the search that had been conducted previously by a private party and therefore," the Court concluded, "it must be characterized as a separate search." *Id.* at 657.

By analogy, the same is true here. The hash value apparently identified by PhotoDNA (like the labeling and drawings in *Walter*), may have provided probable cause, but Sgt. Servat did not bother with a warrant. Instead, he simply viewed the image himself. This was a substantial expansion of the search conducted by Microsoft and NCMEC, and violated the Fourth Amendment.[13] Worse, Here, Sgt. Servat recklessly omitted all of the key facts that the reviewing court would need to assess the legality of his own search and the potentially tainted evidence flowing from it. Namely, Sgt. Servat, omitted: (1) the fact that Microsoft used PhotoDNA to identify the image; (2) any technical or background information whatsoever about PhotoDNA, the rate of false matches, or other errors; (3) any information concerning the process by which Microsoft links flagged images to particular accounts; (4) the apparent fact that no Microsoft employee contemporaneously reviewed the image flagged or other information before it was furnished to law enforcement. Without these details, as a practical matter, the reviewing court simply could not have fairly analyzed the extent to which Sgt. Servat's search exceeded the scope of Microsoft's initial intrusion. *See, e.g., United States v. Wilson*, No. 15-cr-02838, 2017 WL 2733879, at *8-11 (S.D. Cal. Cal. June 26, 2017) (appeal pending) (district court conducting extensive analysis after full evidentiary hearing and concluding, based on the technical details of the technology at issue, that law enforcement's search of child pornography identified by Google's proprietary filtering technology did not constitute a significant expansion of the company's search). This issue is highly fact-specific and will turn on the details of PhotoDNA and Microsoft's review of the evidence in this case. However, what is clear at this stage is that these omissions had the effect of depriving the reviewing court of material facts, and improperly substituting the bare conclusions of Sgt. Servat for the reasons judgment of the Superior Court based on all of the relevant facts. As in *Wilson*, an

[13] Again, should the government seek to defend Sgt. Servat's search as falling within the private search exception, Mr. Bohannon will address that argument on the merits with additional argument and evidence. To do so now, however, would be premature.

evidentiary hearing is warranted.

C. SFPD cannot invoke the good faith exception because the "bare bones" probable cause statement was so facially deficient no reasonable officer would have relied upon it.

In the absence of probable cause, suppression is appropriate here because SFPD cannot carry its burden to establish the good faith exception. No objectively reasonable officer could possibly believe that a warrant application establishes probable cause under controlling law when it (1) fails to relate when or how contraband was discovered, and (2) further fails to justify a delayed search with "good reason" to show why the contraband would likely be stored indefinitely and irrespective of the discovery date in the place to be searched.

Under *United States v. Leon*, 468 U.S. 897 (1984), the evidence should be suppressed unless the government acted in "good faith," *i.e.*, with "objective reasonableness." *Id.* at 913; *Weber*, 923 F.3d at 1346 (same). The government bears the burden of establishing that the good faith exception applies.[14] *United States v. Underwood*, 725 F.3d 1076, 1085 (9th Cir. 2013); *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 706 (9th Cir. 2009) (the government must "prov[e] that officers relied on the search warrant in an objectively reasonable manner") (internal quotation marks omitted). *Leon*'s objective "objective reasonableness" standard "requires officers to have a reasonable knowledge of what the law prohibits." *Id.* at 919-20 n. 20. Although a warrant issued by a judge upon a finding of probable cause is generally presumptively valid, as *Leon* explains, "it is clear that in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." *Id.* at 923.

For example, an officer may not "manifest objective good faith in relying on a warrant based on an affidavit 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.'" *Id.* at 923 (citing *Brown v. Illinois*, 422 U.S. 590, 610-611 (1975)); *see also Gates*, 462 U.S. at 263-64. "An affidavit is so lacking in indicia of probable cause, or bare bones, when it fails to provide a colorable argument for probable cause." *Underwood*, 725 F.3d at 1085 (citing *United States*

[14] Since the government bears the burden and has not yet even raised the issue, Mr. Bohannon reserves the right to make additional arguments and submissions should the government claim good faith.

v. Hove, 848 F.2d 137, 139–40 (9th Cir. 1988)). Similarly, and "depending on the circumstances of the particular case, a warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923 (citing *Massachusetts v. Sheppard*, 468 U.S. 981, 988-991 (1984)). Of course, an officer also cannot in good faith rely on a warrant issued on the basis of reckless omissions in the probable cause statement that constitute a *Franks* violation. *Leon*, 468 U.S. at 423. If any of these situations applies "'need not inquire further'" and can conclude that the good faith exception to the exclusionary rule does not apply." *Underwood*, 470 F.3d at 905.

Under all of these rubrics, the probable cause statement in this case fails by a fair margin. First, as set forth above, the probable cause statement relied on Sgt. Servat's unconstitutional search of the image forwarded by Microsoft and NCMEC, as well as the *Franks* violations outlined above. But even if the Court rejects these arguments, and as set forth above, Sgt. Servat's application is simply not of the type "sufficient to create disagreement among thoughtful and competent judges as to the existence of probable cause." *Leon*, 468 U.S. at 926. Rather, it is precisely the kind of "bare bones" affidavit that the Ninth Circuit and the Supreme Court have repeatedly warned against. *Gates*, 462 U.S. at 239; *Weber*, 923 F.2d at 1346. Nor was reliance possibly reasonable. Quite to the contrary, Sgt. Servat's failure to provide the most basic information, concerning when and how Microsoft discovered an image of child pornography, compounded by his failure to include any "good reasons" why the contraband would still be found in the OneDrive account, clearly violates decades of settled Fourth Amendment jurisprudence from the Ninth Circuit that sets forth the prerequisites for obtaining a warrant for electronically-stored child pornography. *Lacy*, 119 F.3d at 745-46; *Schesso*, 730 F.3d at 1042-43; *Weber*, 923 F.2d at 1346. Put another way, the glaring omission of the date of Microsoft's original discovery and the attendant circumstances renders the warrant application "facially deficient," *Leon*, 468 U.S. at 923, and the further failure to explain why contraband would be stored indefinitely in a paid file-hosting account, *especially without reference to any discovery date*, renders it "so lacking in any indicia of probable cause," that no reasonable law enforcement officer could reasonably rely upon it.

Id. (citing *Brown v. Illinois*, 422 U.S. at 610-611). "[S]imply looking at the affidavit would be sufficient to alert any reasonable officer that probable cause does not exist." *Underwood*, 725 F.3d at 1087.

The defense has been unable to locate any child pornography case in the Ninth Circuit that comes close to presenting such a drastic lapse by law enforcement, let alone one where the validity of the search was upheld. Instead, as noted above, a review of the case law shows that it has been law enforcement's standard practice for many years, and in every case reported, to provide the information that is plainly missing here when applying for a warrant targeting electronically-stored child pornography. Moreover, the Ninth Circuit has rejected the good faith exception in fairly analogous circumstances. For instance, in *Underwood*, the Ninth Circuit rejected the government's good-faith claim because the affidavit did not "set forth a sufficient factual basis for the conclusion[s]" that the defendant was a drug-trafficking courier or that evidence of drug trafficking would be found in his home. *See* 725 F.3d at 1085-86. The only evidence of the defendant's status as a courier was law enforcement's observation of him delivering two crates to known co-conspirators in the drug trade. *Id.* at 1086. The declaration also offered expert averments concerning the tendency of drug traffickers to possess drugs and evidence of their crimes at home. *Id.* The court held that there was insufficient evidence the defendant was a drug courier, and no foundation for the expert testimony concerning the defendant's home—because there was no evidence the defendant was a drug trafficker. *Id.* Here, the sum of the probable cause statement is that a single image of child pornography was uploaded to a file-hosting account at an *unknown* time in the past. As in *Underwood*, that amounts to scant evidence of a crime, and provides no grounds to conclude that the *current* contents of the account would likely reveal contraband or evidence of a crime. As in *Underwood*, the warrant application here fails to present a "colorable argument for probable cause," well beyond the point where "thoughtful and competent" legal minds might disagree. *Id.* at 1085.

Finally, policy considerations also counsel in favor of suppression. As *Leon* and its progeny explain, the "primary purpose" of the exclusionary rule is "to deter law enforcement from carrying out

unconstitutional searches and seizures." *Underwood*, 725 F.3d at 1084. And "[a]lthough the exclusionary rule is often framed as a nuisance to law enforcement, [the Ninth Circuit] view[s] it as a promoter of police professionalism and education." *Id.* at 1084-85 (citing *Herring v. United States*, 555 U.S. 135, 156 n. 6 (2009) (Ginsburg, J., dissenting) (noting that "professionalism is a sign of the exclusionary rule's efficacy ….")). We require relatively little of law enforcement when it comes to authoring search warrants, but the probable cause statement at issue here does not even clear that low bar. This is simply not a case where law enforcement's conduct was "objectively reasonable and largely error-free." *Sheppard*, 468 U.S. at 990. Nor is it a case where the errors may be attributed to another officer's negligence in bookkeeping and attenuated from the challenged arrest, as in in *United States v. Herring*, 555 U.S. 135, 137 (2009). This was, rather, gross negligence by Sgt. Servat concerning glaring omissions that are basic to establishing probable case under any reasonable understanding of the law—mistakes that led directly to the violation of Mr. Bohannon's rights. *See United States v. Camou*, 773 F.3d 932, 945 (9th Cir. 2014) ("The Supreme Court has never applied the good faith exception to excuse an officer who was negligent himself, and whose negligence directly led to the violation of the defendant's constitutional rights."). As the Ninth Circuit explained in *United States v. Lopez–Soto*, "there is no good-faith exception to the exclusionary rule for police who do not act in accordance with governing law." 205 F.3d 1101, 1106 (9th Cir. 2000). "To create [such] an exception ... would defeat the purpose of the exclusionary rule, for it would remove the incentive for police to make certain that they properly understand the law that they are entrusted to enforce and obey." *Id.*; *see also United States v. Song Ja Cha*, 597 F.3d 995, 1005 (9th Cir. 2010) (same).

In sum, the good-faith exception does not apply because the warrant was fatally deficient on its face and fell far short of establishing probable cause under any reasonable understanding of the law.

\\

\\

\\

\\

IV. CONCLUSION

For all these reasons, Mr. Bohannon respectfully requests that the Court grant his motion to suppress.

Dated: October 14, 2020

Respectfully submitted,

STEVEN G. KALAR
Federal Public Defender
Northern District of California

/S
DAVID W. RIZK
Assistant Federal Public Defender